

Notes (02/28/2024)

Tips for Preventing Cybercrimes

1. **Email Spoofing:**
 - Enable email authentication protocols like SPF, DKIM, and DMARC to verify email sources.
2. **Phishing:**
 - Always double-check email sender addresses and avoid clicking on suspicious links; verify with the organization directly.
3. **Spear Phishing:**
 - Be cautious with sharing personal information online; double-check emails for personalized details before responding.
4. **Vishing:**
 - Avoid sharing sensitive information over the phone; verify the caller's identity and call back using official contact information.
5. **Smishing:**
 - Don't click on links or respond to text messages from unknown sources; verify with the organization through official channels.
6. **Spamming:**
 - Use spam filters on email accounts and avoid clicking on or responding to unsolicited emails.
7. **Cyber Defamation:**
 - Think before posting online; avoid spreading false information about individuals or organizations.
8. **Cyberstalking:**
 - Adjust social media privacy settings and be cautious about sharing location details online.
9. **Computer Sabotage:**
 - Regularly update and patch software to protect against vulnerabilities.
10. **Pornographic Offenses:**
 - Be cautious when accessing online content; use reputable websites and avoid illegal downloads.
11. **Password Sniffing:**
 - Use strong, unique passwords and enable two-factor authentication for added security.
12. **Credit Card Fraud:**
 - Regularly monitor bank statements; report any unauthorized transactions immediately.
13. **Piracy:**
 - Avoid downloading or sharing copyrighted content without permission.

14. Internet Time Theft:

- Manage time efficiently and avoid unauthorized use of work hours for personal activities.

15. Unauthorized Accessing of Computer:

- Use strong passwords, encrypt sensitive data, and restrict access to authorized users.

16. DoS Attack:

- Implement network security measures and use a firewall to protect against denial-of-service attacks.

17. Virus Attack:

- Install reputable antivirus software and keep it up to date; be cautious with email attachments.

18. Email Bombing:

- Use email filters and report suspicious email activity to your email provider.

19. Salami Attack:

- Monitor financial transactions regularly for small, unauthorized deductions.

20. Logic Bomb:

- Be cautious with downloading files from unknown sources; keep software updated.

21. Trojan Horse:

- Avoid downloading files from untrusted sources; use reputable security software.

22. Data Diddling:

- Regularly check and verify data integrity to detect any unauthorized changes.

23. Software Piracy:

- Use licensed software and avoid downloading cracked versions.

24. Cyberterrorism:

- Stay informed about potential cyber threats and report suspicious online activity.

25. Forgery:

- Verify the authenticity of digital signatures and digital documents.

26. Web Jacking:

- Regularly monitor and update website security protocols.

27. Crimes Emanating from User Network Newsgroup:

- Be cautious about sharing sensitive information in online forums; use secure, private channels when necessary.

Also view at <https://sites.google.com/view/owca/notes/02-28-2024>